IN THE UNITED STATES PATENT and TRADEMARK OFFICE

Inventors:	Yigal Mordechai Edery, Nimrod Itzhak Vered, David R Kroll, Shlomo Touboul	Control No.: Unassigned
Patent No.:	8,079,086	
Issue Date:	Dec. 13, 2011	
Filing Date:	May 26, 2009	
Title:	MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS	

Mail Stop Ex Parte Reexam
Central Reexamination Unit
Office of Patent Legal Administration
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

ATTACHMENT TO REQUEST FOR EX-PARTE REEXAMINATION (FORM PTO-SB/57; PTO-1465) PROVIDING INFORMATION ON U.S. PATENT NO. 8,079,086

Reexamination under 35 U.S.C. §§ 302-307 and 35 C.F.R. § 1.510 is respectfully requested of United States Patent No. 8,079,086 (the "Edery 086 patent"), which was filed on May 26, 2009 and issued on December 13, 2011. The Edery 086 patent is enforceable and reexamination is appropriate under 37 C.F.R. § 1.510(a). The Edery 086 patent currently is being asserted in the patent infringement case styled *Finjan, Inc. v. FireEye, Inc.*, 13-cv-3133 (N.D. Cal.).

I. CLAIMS FOR WHICH REEXAMINATION IS REQUESTED

Reexamination is requested of claims 1, 2, 3, 4, 5, 6, 7, 8, 17, 18, 19, 20, 21, 22, 23, 31, 32, 35, 36, 39 and 41of the Edery 086 patent.

II. CITATION OF PRIOR ART

The Edery 086 patent was filed on May 26, 2009 as application No. 12/471,942 (the "942 application"). It is a continuation of and claims priority to U.S. Patent No. 7,613,926 to Edery ("Edery 926"), filed on March 7, 2006, which is a continuation of U.S. Patent No. 7,058,822 to Edery ("Edery 822"), which was filed on May 17, 2001.

Requester seeks reexamination of the Edery 086 patent in light of the combination of U.S. Patent No. 5,983,348 to Ji (the "Ji patent") and U.S. Patent No. 6,092,194 to Touboul (the "Touboul 194 patent"). The Ji patent was filed on September 10, 1997 and issued on November 9, 1999. The Touboul 194 patent was filed on November 6, 1997 and issued on July 18, 2000. Thus, the Ji patent in combination with the Touboul 194 patent is prior art to the Edery 086 patent under 35 U.S.C. § 103(a). The Touboul 194 patent was not substantively considered during the examination of the Edery 086 patent, either alone or in combination with the Ji patent. Because the combination of the Ji patent and the Touboul 194 patent was not substantively considered by the examiner, this combination provides a new ground for examination. As more thoroughly discussed below, the new ground for examination coupled with the disclosure of all elements of claims 1, 2, 3, 4, 5, 6, 7, 8, 17, 18, 19, 20, 21, 22, 23, 31, 32, 35, 36, 39 and 41 by the combination of the Ji patent and the Touboul 194 patent constitutes a substantial new question of patentability.

III. STATEMENT POINTING OUT SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY

The Ji patent in combination with the Touboul 194 patent establishes a substantial new question of patentability of claims 1, 2, 3, 4, 5, 6, 7, 8, 17, 18, 19, 20, 21, 22, 23, 31, 32, 35, 36, 39 and 41 of the Edery 086 patent.[1] The substantial new question of patentability meets the legal standard for ordering *ex parte* reexamination as set forth in the MPEP § 2216:

> It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.

The combination of the Ji patent and the Touboul 194 patent includes the requisite elements in the claims of the Edery 086 patent for which reexamination is requested. Therefore, the Office should grant this request.

[1] The Ji patent alone constitutes prior art under 35 U.S.C. § 102(e), but for purposes of this reexamination, Requester presents the referenced § 103 combination of the Ji patent and the Touboul 194 patent.

A. Background of the Edery 086 Patent

Generally, the Edery 086 patent relates to a computer processor-based method that, according to claim 1, includes: (1) receiving a downloadable, (2) deriving security profile data for the downloadable that includes a list of suspicious computer operations the downloadable may attempt, (3) appending the downloadable with a representation of the downloadable security data, and (4) transmitting the appended downloadable to a destination computer.

More specifically, the Edery 086 patent relates to protection systems and methods capable of protecting network accessible devices or processes from malicious operations. The disclosed embodiments provide for determining whether received information from a third party includes executable code. The Edery 086 patent provides for determining, within one or more network servers, whether a received downloadable includes executable code. Additionally, the embodiments provide for a protection engine that operates within one or more network servers, firewalls, or other network connectable information devices. The protection engine itself includes an information monitor for monitoring the information received by the server. A code detection engine determines whether any of the information received by the server includes executable code.

Furthermore, the embodiments disclosed in the Edery 086 patent contemplate "delivering static, configurable and/or extensible remotely operable protection policies to a Downloadable-destination, more typically as a sandboxed package including the mobile protection code, downloadable policies and one or more received Downloadables." Edery 086 at Col. 2, lines 55-59. The embodiments further disclose causing the mobile protection code to be executed within the destination, which could include a web browser, in a manner that enables the downloadable operations to be detected, intercepted, or further responded to via the various protected operations. Edery 086 at Col. 3, lines 32-50.

The methods disclosed in independent claims 1, 17, 31, 35, 39 and 41 are depicted in Figure 9 of the Edery 086 patent:

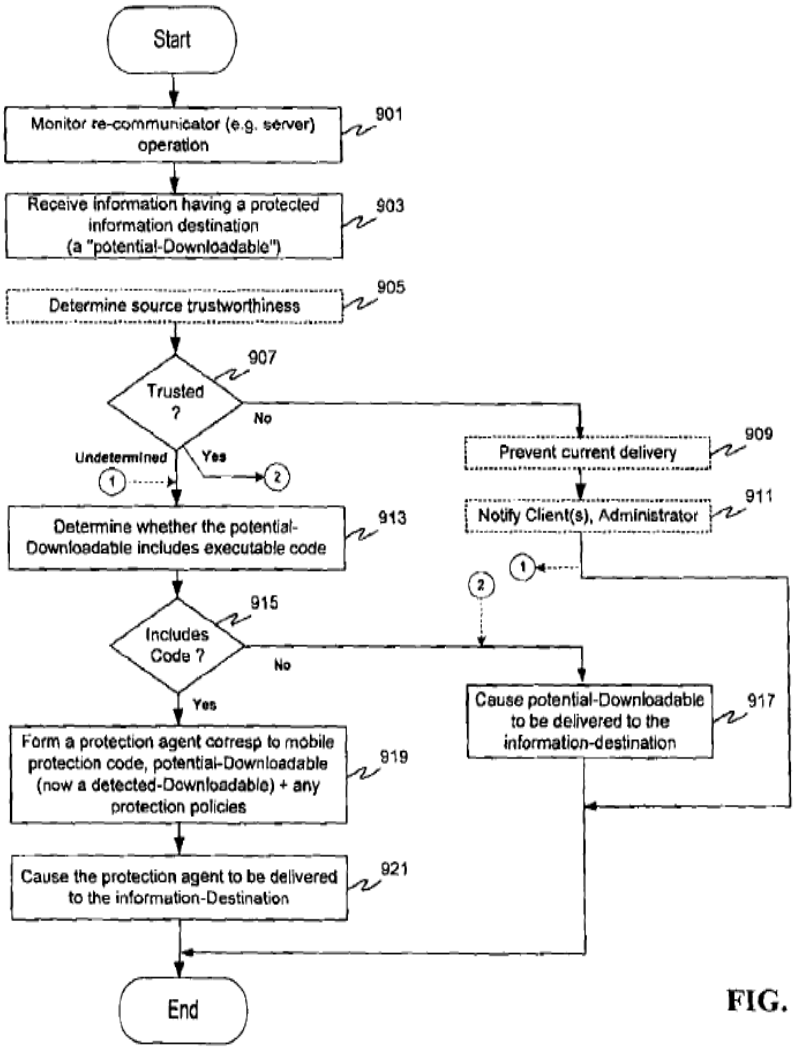

FIG. 9

In addition to the aforementioned embodiments, the method set forth in claim 1 involves a computer receiving downloadable information, deriving security profile data for the Downloadable and appending a representation of the Downloadable security data to the Downloadable to generate an appended Downloadable before transmitting the appended Downloadable to a third device, such as a computer.

B. The Examination of the Edery 086 Patent

The Edery 086 patent was prosecuted as the 942 application. On May 26, 2009, in response to an outstanding Office Action of February 25, 2009 in the co-pending parent application, U.S. Serial No. 11/370,114, the applicants filed a preliminary amendment adding claims of priority to (1) the Edery 822 patent, (2) U.S. Patent No. 6,804,780 ("Touboul 780"), (3) the Touboul 194 patent, and (4) U.S. Patent No. 6,480,962 ("Touboul 962"). May 26, 2009 Preliminary Amendment at p. 2. The preliminary amendment also designated the 942

application as a continuation of application U.S. Serial No. 11/370,114, which was a continuation of U.S. Serial No. 09/861,229, which matured into Edery 822. *Id*. at pp. 2-3. The preliminary amendment additionally cancelled pending claims 1-76 and added new claims 77-136. *Id*. at pp. 3-16.

In the preliminary amendment, the applicants also argued that the Ji patent, filed on September 10, 1997, was inadmissible prior art. *Id*. at p. 18. The applicants contended that the 942 application was a continuation of U.S. Serial No. 11/370,114, which was a continuation of U.S. Serial No. 09/861,229 (now U.S. Patent No. 7,058,822), which was a continuation-in-part of U.S. Serial No. 09/539,667 (now U.S. Patent No. 6,804,780), which was a continuation of U.S. Serial No. 08/964,388 (now U.S. Patent No. 6,092,194), which claims priority to provisional application U.S. Serial No. 60/030,639, filed on November 8, 1996. *Id*. at pp. 18-19. The applicants further contended that the pending claims were supported by U.S. Serial No. 60/030,639. *Id*. at p. 19. However, as demonstrated below, the applicants dropped this argument and did not refute the examiner's assertion that the 942 application could not claim priority to the provisional application U.S. Serial No. 60/030,639.

In the preliminary amendment, the applicants also argued that the claimed invention was not anticipated or rendered obvious by the Ji patent because: "(i) Ji does not disclose a Downloadable security profile database, and (ii) Ji does not disclose appending a security profile of a Downloadable to a Downloadable." *Id*. at p. 19. Therefore, the applicants limited the alleged novelty of the 942 application to these two discrete points. The applicants described their invention as "relat[ing] to a Downloadable security scanner that operates by deriving or retrieving a security profile for a Downloading, and transmitting the Downloadable and a representation of the security profile to a receiver computer." *Id*. The applicants further stated that: "The security profile [itself] includes a list of suspicious computer operations that may be performed by the Downloadable," and "the representation of the security profile may be appended to the Downloadable." *Id*. The applicants further stated that the receiver computer in turn reviews the security profile and decides based on the security profile whether or not to execute the Downloadable and, "if so, whether or not to execute the Downloadable in a controlled manner or environment." *Id*.

The applicants stated that the Ji patent, on the other hand, "describes an applet security scanner that operates by identifying suspicious function calls in an applet, and inserting a first

instruction sequence, before a suspicious function call, and inserting a second instruction sequence, after the suspicious function call." *Id*. at pp. 19-20. The applicants stated that, in the Ji patent, "the first instruction sequence generates a call to a pre-filter function, with the name of the suspicious function and possibly other data as pre-filter function parameters." *Id*. at p. 20. The applicants stated that, in the Ji patent, "[t]he second instruction sequence generates a call to a post-filter function, with the result of the suspicious function invocation and possibly other data as post-filter function parameters." *Id*.

The applicants argued that, given their characterization of the Ji patent, the Ji patent did not disclose a downloadable security profile database by relying on prior art cited by the Ji patent and disclosed in the priority document U.S. Serial No. 60/030,639 relating to prior technology in a product termed SurfinGate. *Id*. The applicants cited this prior art as purported evidence that the Ji patent did not disclose a downloadable security profile database, because the Ji patent states in Col. 2, lines 32 and 33 that "SurfinGate maintains an applet profile database." *Id*. The applicants also argued that "Ji does not disclose appending a security profile of a downloadable to a downloadable." *Id*. at 21. The applicants attempted to distinguish the Ji patent by arguing that it "discloses alteration of a downloadable, referred to in Ji as '*instrumentation*', to disable suspicious operations." *Id*. (emphasis in original). The applicants described their claimed invention as:

> [A]ppend[ing] a list of suspicious operations in the form of a security profile to a downloadable, for a receiver thereof to decide how to respond thereto. One receiver may allow the downloadable to execute, in response to the security profile, yet another receiver may block it.

Id. To attempt to distinguish the Ji patent, the applicants argued that "[w]hereas Ji takes an instrumentation action to disable suspicious operations, the claimed invention provides a report about the suspicious operations." *Id*. The applicants then replied substantively to the February 2009 Office Action in the co-pending parent application U.S. Serial No. 11/370,114 that the Ji patent was purportedly distinguishable from the 942 application for the reasons set forth above. *Id*. at pp. 21-27.

On September 20, 2010, in response to the May 26, 2009 preliminary amendment, the examiner issued an Office Action rejecting pending claims 77-136. The examiner rejected the terminal disclaimer, which disclaimed any portion of the patent beyond the expiration date of

U.S. Patent Nos. 6,092,194, 6,154,844, and 6,804,780, because the disclaimer was signed by an improper party. Sept 20, 2010 Office Action at pp. 2-3. The examiner also rejected pending claims 77-136 on the grounds of nonstatutory obviousness-type double patenting over claims 1-30 of U.S. Patent No. 7,613,926, claims 1-35 of U.S. Patent No. 6,480,962, claims 1-8 of U.S. Patent No. 6,167,520, claims 1-41 of U.S. Patent No. 7,647,633, claims 1-18 of U.S. Patent No. 6,804,780, claims 1-44 of U.S. Patent No. 6,154,844, and claims 1-68 of U.S. Patent No. 6,092,194.

The examiner also rejected pending claims 77-136 under 35 U.S.C. § 102(e) as being anticipated by the Ji patent. Regarding claim 77, the examiner stated that the Ji patent teaches "a computer-based method, comprising the steps of receiving an incoming Downloadable; deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and storing the Downloadable security profile data in a database (col. 3, lines 32-56 and col. 6, lines 38-51)." *Id*. at pp. 6-7. The examiner then described how each of the pending claims were anticipated by the Ji patent. *Id*. at 7-13.

On December 20, 2010, the applicants responded to the September 2010 Office Action, arguing the claimed invention was patentable over the Ji patent. Dec. 20, 2010 Response at pp. 17-26. The applicants amended claims 113, 114, 116, 117, 120, 121, 123 and 124 "to more properly claim the present invention" without allegedly introducing new matter. *Id*. at p. 16. The applicants also argued that the examiner "did not consider applicants' arguments" from their May 26, 2009 preliminary amendment. *Id*. at p. 17. The applicants then repeated their arguments from the May 26, 2009 preliminary amendment and applied those arguments to pending claims 77-136. *Id*. at pp. 17-25.

On June 15, 2011, the examiner issued a Final Office Action rejecting pending claims 77-136, finding that the examiner's objections to the pending claims had been overcome. As to the rejections issued by the examiner, the examiner found that the applicants' arguments "have been fully considered but they are not persuasive." June 15, 2011 Office Action at p. 2. The examiner disagreed that provisional application U.S. Serial No. 60/030,639 provided support for the claims in the 942 application and requested a specific showing in the provisional application to prove support for the priority date of November 8, 1996. *Id*.

Regarding pending claims 77-94, the examiner noted that the features relied upon by the applicants to distinguish the prior art were not recited in rejected claims 77-94. The examiner

stated that "Ji discloses of a downloadable security profile database, the teachings recite of sending reports back to a server (containing a database) which include a list of suspicious operations that may be attempted by the downloadable, see column 6, lines 38-51." *Id*. at 3. The examiner also rejected pending claims 77-136 for non-statutory obviousness-type double patenting as being unpatentable over claims 1-30 of U.S. Patent No. 7,613,926, claims 1-35 of U.S. Patent No. 7,480,962, claims 1-8 of U.S. Patent No. 6,167,520, and claims 1-41 of U.S. Patent No. 7,647,633.

The examiner again rejected pending claims 77-94 under 35 U.S.C. 102(e) as being anticipated by the Ji patent, finding:

> As per claim 77, it is taught of a computer based method, comprising the steps of receiving an incoming Downloadable; deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and storing the Downloadable security profile data in a database (col. 3, lines 32-56 and col. 6, lines 38-51).

Id. at p. 7. The examiner identified similar reasons and citations as the quoted language above to the Ji patent, demonstrating how the Ji patent anticipated the remaining pending claims 77-94 of the 942 application. *Id*. at pp. 7-8. The examiner allowed pending claims 95-136, but noted the rejections under obvious-type double patenting.

On July 19, 2011, the applicants responded by cancelling claims 77-94 and filing a terminal disclaimer to overcome the obvious-type double patenting rejections. July 11, 2011 Response at p. 2. The applicants did not, however, address the examiner's conclusion that the 942 application could not claim priority to provisional application U.S. Serial No. 60/030,639.

On August 10, 2011 the examiner issued a Notice of Allowance. On December 13, 2011, the 942 application issued as the Edery 086 patent.

C. SNQP – The Ji Patent In View of the Touboul 194 patent raises a SNQP as to Claims 1, 2, 3, 4, 5, 6, 7, 8, 17, 18, 19, 20, 21, 22, 23, 31, 32, 35, 36, 39, and 41 under 37 CFR 1.510(b)(1)

The combination of the Ji patent and the Touboul 194 patent raises a SNQP as to the requested claims, because the two references disclose the exact limitations that the applicants argued were not present in the prior art. The *KSR International Co. v. Teleflex Inc.* obviousness standard[2] dictates that the teachings from the Ji and Touboul 194 patents related to the system

[2] In *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398, 415 (2007), the Supreme court

and methods for protecting network-connectible devices from undesirable downloadable operations are properly combinable and representative of the obvious body of knowledge within the grasp of the average practitioner skilled in the art of computer network protection. One of ordinary skill in the art would be motivated to combine these references, because the Ji patent and the Touboul 194 patent are directed to very similar technology. *See* Ji at 1:66-2:42; Touboul 194 at 1:24-2:37. Indeed, the specification of the Ji patent discloses technology in the art that the Touboul 194 patent allegedly covered. *See* Ji at 1:66-2:42.

As discussed above, the applicants argued that the points of novelty of the Edery 086 patent are: (i) a Downloadable security profile database, and (ii) appending a security profile of a Downloadable to a Downloadable. *See* May 26, 2009 Preliminary Amendment at pp. 19-20. However, the combination of the Ji patent and the Touboul 194 patent disclose both of these elements.

The Ji patent discloses appending a security profile of a downloadable to a downloadable. Ji at 3:31-44, 4:43-54, 5:21-6:51, and 7:44-8:5. The Ji patent's disclosure of this element is particularly evident in column 5, lines 21-27: "If an instruction (a suspicious instruction) that calls an insecure function (as determined by a predefined set of functions) is found during this static scanning, a first instruction sequence (pre-filter) is inserted before that instruction and a second instruction sequence (post-filter) after that instruction by the instruments." Further, the Ji patent discloses downloading and detecting the downloadable security profile data contained in the "dependency" Java class files required by the downloadable during execution, appending these files to the downloadable, and delivering them as "a single JAR (Java archive) file" to the client computer. Ji at 6:38-42, 7:8-28.

The Touboul 194 patent discloses a downloadable security profile database in Figures 2 and 3 and their accompanying text in column 3 line 23 to column 7 line 6. The Touboul 194 patent discloses the Downloadable Security Profile (DSP) database in column 3 lines 47-50: "The data storage device 230 stores a security database 240 which includes security information

---

"beg[a]n by rejecting the rigid approach of the Court of Appeals (i.e., requiring satisfaction of the "teaching, suggestion, motivation" (TSM) test) to show an invention would have been obvious (and is therefore unpatentable). Returning to its own nonobviousness cases, the Court held that "the [nonobviousness] analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ." *Id*. at 418.

for determining whether a received Downloadable is to be deemed suspicious." Additionally, the Touboul 194 patent discloses the DSP database in column 4 lines 14-18: "The security program 255 operates in conjunction with the security database 240, which includes security policies 305, known Downloadables 307, known Certificates 309 and Downloadable Security Profile (DSP) data 310 corresponding to the known Downloadables 307." Figure 2 of the Touboul 194 patent depicts the disclosed DSP database as item 240, while Figure 3 depicts the DSP database at item 240, the DSP data as item 310 and the security policies as item 305:

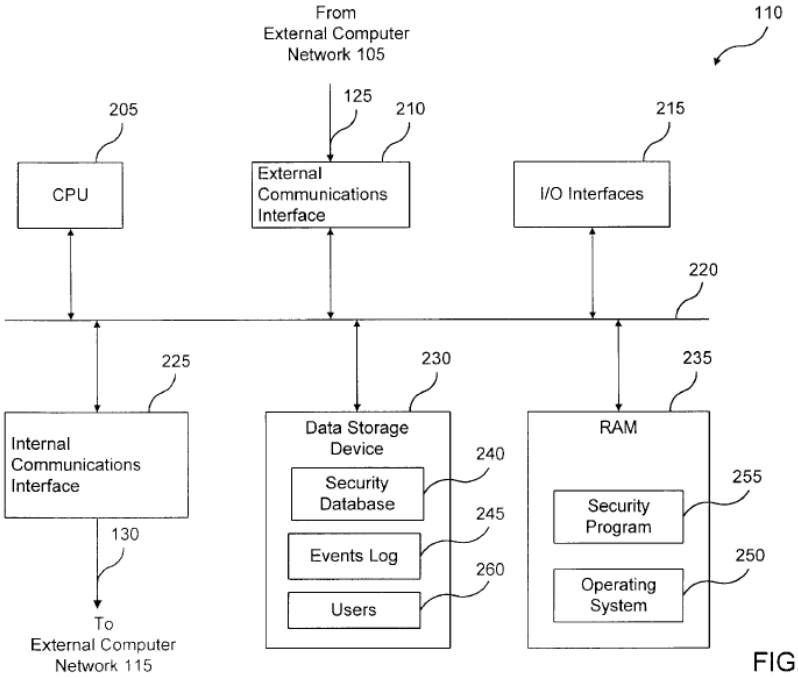

FIG. 2

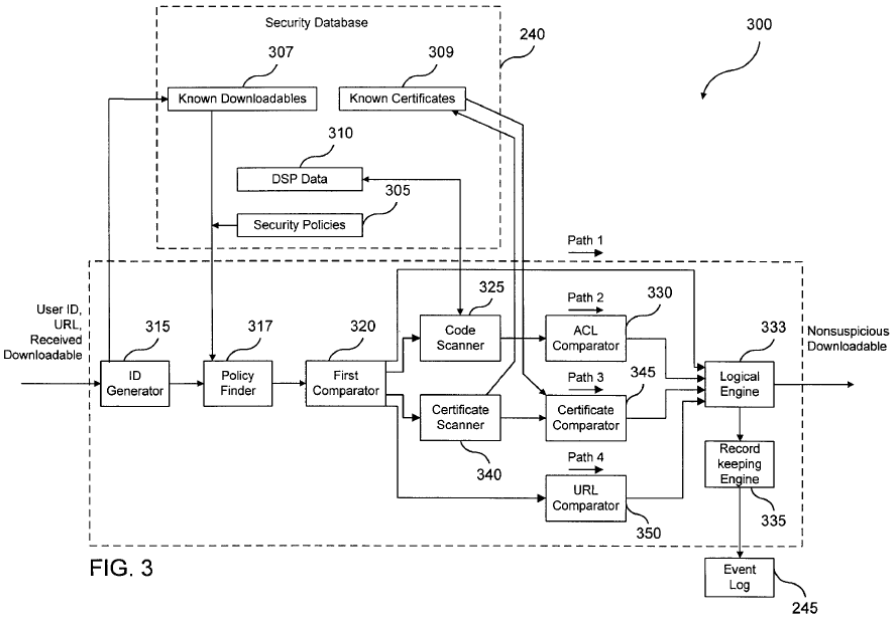

FIG. 3

Accordingly, the two elements that the applicants argued did not exist in the prior art are clearly disclosed in the combination of the Ji patent and the Touboul 194 patent, and this combination raises a substantial new question of patentability not previously considered by the examiner. *See In re Swanson*, 540 F.3d 1368, 1380 (Fed. Cir. 2008) ("the PTO should evaluate the context in which the reference was previously considered and the scope of the prior consideration and determine whether the reference is now being considered for a substantially different purpose").

D. The Edery 086 Patent Is Not Entitled to a Priority Date From The Alleged Parent Continuation-In-Part Patents.

As discussed above in Section III.B., the Edery 086 patent cannot claim priority to any document filed before the Edery 822 patent's filing of May 17, 2001. As the MPEP explains, determination of the proper priority date is appropriate as part of a request for *ex parte* reexamination:

> The statement applying the prior art may, where appropriate, point out that claims in the patent for which reexamination is requested are entitled only to the filing date of that patent and not supported by an earlier foreign or United States patent application whose filing date is claimed. For example, even where a patent is a continuing application under 35 U.S.C. 120, the effective date of some of the claims could be the filing date of the child application which resulted in the patent, because those claims were not supported in the parent application.

MPEP § 2617.

In the June 15, 2011 Office Action, the examiner considered the applicants' arguments that the Edery 086 patent could claim priority to provisional application U.S. Serial No. 60/030,639, but ultimately, the examiner correctly found that the applicants could not claim priority to the provisional application. June 15, 2011 Office Action at p. 2. The applicants later responded to the June 15, 2011 Office Action on other grounds but did not address the examiner's rejection of the applicants' claim to priority. Accordingly, the applicants failed to demonstrate that the Edery 086 patent could claim priority earlier than May 17, 2001. This failure establishes the Edery 086 priority date of not earlier than May 17, 2001.

Moreover, as illustrated below, although the Edery 086 patent attempts to claim priority to U.S. Patent Nos. 6,480,692 and/or 6,804,780, the claims of the Edery 086 patent are "not supported" in those specifications. See U.S. Patent Nos. 6,480,692 and 6,804,780. Accordingly, the applicable priority date for purposes of the invalidity analysis is not earlier than May 17, 2001.

The following portions of the Edery 086 patent (and the Edery 822 patent) were all "new matter" in the CIP application:

- FIG. 1a
- FIG. 1b
- FIG. 1c
- FIG. 2
- FIG. 3
- FIG. 4
- FIG. 5
- FIG. 6a
- FIG. 6b
- FIG. 7a
- FIG. 7b
- FIG. 8
- FIG. 9
- FIG. 10a
- FIG. 10b
- FIG. 11
- FIG. 12a
- FIG. 12b and
- Col. 1:55 thru Col. 24:3

Consequently, all of the descriptions constitute new matter first introduced on May 17, 2001 with the filing of the Edery 822 patent. Similarly, all of the descriptions and claim limitations relating to the aforementioned, including but not limited to appending the security profile data to the downloadable and transmitting the appended downloadable to a destination

computer are new matter first introduced on May 17, 2001 with the filing of the Edery 822 patent.

Because the claim scope depends on the newly added material, claims 1, 2, 3, 4, 5, 6, 7, 8, 17, 18, 19, 20, 21, 22, 23, 31, 32, 35, 36, 39 and 41 may only receive the benefit of priority to the May 17, 2001 filing date. See, e.g., *Waldemar Link, GmbH & Co. v. Osteonics Corp.*, 32 F.3d 556, 558 (Fed. Cir. 1994). Therefore, the Ji patent and the Touboul 194 patent properly serve as prior art because their disclosures predate the claimed subject matter of the Edery 086 patent.

IV. EXPLANATION OF PERTINENCY AND MANNER OF APPLYING CITED PRIOR ART TO EVERY CLAIM FOR WHICH REEXAMINATION IS REQUESTED UNDER 37 C.F.R. 1.510(B)(2)

A. The Ji Patent In View Of The Touboul 194 Patent

Claims 1, 2, 3, 4, 5, 6, 7, 8, 17, 18, 19, 20, 21, 22, 23, 31, 32, 35, 36, 39 and 41 are obvious under 35 U.S.C. § 103(a) in light of Ji patent in view of the Touboul 194 patent. The claim chart below details the manner of applying the Ji and Touboul 194 patents to every claim of the Edery 086 patent for which reexamination is requested.

As discussed above, the Edery 086 patent is not entitled to a priority date earlier than May 17, 2001. The Ji patent was filed on September 10, 1997. The Touboul 194 patent was filed on November 6, 1997. Accordingly, the combination of the Ji patent and the Touboul 194 patent is prior art to the Edery 086 patent under 35 U.S.C. § 103(a).

Additionally, a person of ordinary skill would be motivated to combine the Ji patent with the teachings of the Touboul 194 patent because the Touboul 194 patent, like the Ji patent (at 1:3-6), is directed toward detecting and blocking computer viruses and other malicious code attacks. Touboul 194 Abstract; 1:23-27.

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
1. A computer-based method, comprising the steps of:	The Ji patent discloses the preamble. Ji discloses computer implemented applications executing on a computer network. Specifically, the Abstract discloses a "network scanner for security checking of application programs […] received over the Internet or an Intranet has both static (pre-run time) and dynamic (run time) scanning. […] During run time at the client, the instrumented instructions are thereby monitored for security policy violations, and execution of an instruction is prevented in the event of such a violation."

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
	Figure 1 of the Ji patent discloses a server and client computer device. It is well understood that a computer includes one or more processors for executing software applications.
receiving an incoming Downloadable;	The Ji patent discloses the step of receiving an incoming downloadable. The Ji patent discloses receiving files "(e.g. Java applets or ActiveX controls)" from the Internet at the server in Fig. 1. See also Ji patent at 3:17-23 ("Thereby in accordance with the invention a scanner (for a virus or other malicious code) provides both static and dynamic scanning for application programs, e.g. Java applets or ActiveX controls. The applets or controls (hereinafter collectively referred to as applets) are conventionally received from e.g. the Internet or an Intranet at a conventional server.").
deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable;	The Ji patent discloses deriving security profile data for the downloadable, including a list of suspicious computer operations that may be attempted by the downloadable. The Ji patent discloses scanning the downloaded file to identify "suspicious instructions" (Ji at 5:22) contained in the downloadable as it is received at the server. Ji at 5:16-6:37. Accordingly, this instrumentation (deriving) identifies specific applet instructions deemed to be "suspicious" (computer operations) as determined by "a predefined set of [insecure] functions." Ji at 5:22-23. Moreover, during the instrumentation process, all potentially suspicious computer operations are identified and listed because the Ji patent discloses a process whereby all Java class files that may be called by the downloadable are scanned and instrumented: "An applet pre-fetcher component 38 fetches from the Internet 10 all the dependency files required by a Java class file, if they are not already packed into a JAR file. This is important because the goal is to attach the scanner monitor package to a session only once. A Java applet may contain more than one code module, or class file. Heretofore this disclosure has assumed that all the class files are packed in one JAR file and downloaded once. One monitoring package is attached to the JAR file and every instantiation of this package on the client web browser 22 marks a unique session. However, if the class files are not packed together and are downloaded on an as-needed basis during applet execution, multiple instrumentation will occur and multiple instances of the monitoring package for the same session are created on the client.

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
	This creates a problem of how to maintain information on session states. To solve this problem, the pre-fetcher 38 pre-fetches the dependency class files during the static scanning of the main applet code module. The dependency class files are (see below) instrumented once, packed together, and delivered to the client." Ji at 7:8-28. Additionally, it would have been obvious to combine the disclosures of the Ji patent with the teachings in the Touboul 194 patent relating to deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable. The Touboul 194 patent teaches deriving downloadable security profile data: "[…] the code scanner 325 resolves the DSP data 310. That is, the code scanner 325 uses conventional parsing techniques to decompose the code (including all prefetched components) of the Downloadable into the DSP data 310. DSP data 310 includes the list of all potentially hostile or suspicious computer operations that may be attempted by a specific Downloadable 307, and may also include the respective arguments of these operations." Touboul 194 at 5:41-48.
appending a representation of the Downloadable security profile data to the Downloadable, to generate an appended Downloadable; and	The Ji patent discloses the step of appending a representation of the Downloadable security profile data to the Downloadable, to generate an appended Downloadable. Specifically, the Ji patent discloses generating the amended downloadable by instrumenting (appending) all of the "suspicious instructions" (downloadable security profile data) in the applet (downloadable). Ji at 5:16-6:37. Additionally, the Ji patent discloses at 7:8-28 (1) downloading "dependency" Java class files not included in the applet (downloadable) but required by the applet during execution; (2) instrumenting the newly downloaded Java class files to derive suspicious instructions (downloadable security profile data) included therein; and (3) appending to the downloadable the instrumented Java class files: "**An applet pre-fetcher component 38 fetches from the Internet 10 all the dependency files required by a Java class file**, if they are not already packed into a JAR file. This is important because the goal is to attach the scanner monitor package to a session only once.

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
	A Java applet may contain more than one code module, or class file. Heretofore this disclosure has assumed that all the class files are packed in one JAR file and downloaded once. One monitoring package is attached to the JAR file and every instantiation of this package on the client web browser 22 marks a unique session. However, if the class files are not packed together and are downloaded on an as-needed basis during applet execution, multiple instrumentation will occur and multiple instances of the monitoring package for the same session are created on the client. This creates a problem of how to maintain information on session states. To solve this problem, **the pre-fetcher 38 pre-fetches the dependency class files during the static scanning of the main applet code module. The dependency class files are (see below) instrumented once, packed together, and delivered to the client.**" Ji at 7:8-28 (emphasis added). The Ji patent further explains that, as depicted in Fig. 1, the security monitoring package and security policies are included with the instrumented downloadable (and the instrumented Java class files) "in a single JAR (Java archive) file format at the server **32**, and downloaded to the web browser **22** in client machine **14**." Ji at 6:38-42.
transmitting the appended Downloadable to a destination computer.	The Ji patent discloses the step of transmitting the instrumented applet (appended downloadable) to the destination computer. After the applet code has been instrumented at the server, "[t]he instrumented applet is then downloaded from the server to the client (local computer), at which time the applet code is conventionally interpreted by the client Web browser and it begins to be executed. As the applet code is executed, each instrumented instruction is monitored by the Web browser using a monitor package which is part of the scanner and delivered to the client side. Upon execution, each instrumented instruction is subject to a security check. If the security policy (which has been pre-established) is violated, that particular instruction which violates the security policy is not executed, and instead a report is made and execution continues, if appropriate, with the next instruction." Ji at 3:32-44. The Ji patent explains that, as depicted in Fig. 1, the security monitoring package and security policies are included with the

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
	instrumented downloadable "in a single JAR (Java archive) file format at the server **32**, and downloaded to the web browser **22** in client machine **14**." Ji at 6:38-42.
2. The computer-based method of claim 1 wherein the Downloadable includes an applet.	The Ji patent discloses the method step wherein the Downloadable includes an applet. "Thereby in accordance with the invention a scanner (for a virus or other malicious code) provides both static and dynamic scanning for application programs, e.g. **Java applets** or ActiveX controls. The applets or controls (hereinafter collectively referred to as applets) are conventionally received from e.g. the Internet or an Intranet at a conventional server." Ji at 3:16-22 (emphasis added).
3. The computer-based method of claim 1 wherein the Downloadable includes an active control.	The Ji patent discloses the method step wherein the Downloadable includes an active control. "Thereby in accordance with the invention a scanner (for a virus or other malicious code) provides both static and dynamic scanning for application programs, e.g. Java applets or **ActiveX controls**. The applets or controls (hereinafter collectively referred to as applets) are conventionally received from e.g. the Internet or an Intranet at a conventional server." Ji at 3:16-22 (emphasis added).
4. The computer-based method of claim 1 wherein the Downloadable includes program script.	It would have been obvious to include scanning for program script (e.g., Java Script or Visual Basis script) to one of ordinary skill in the art because Java and Java Script are closely related. Moreover, it would have been obvious to combine the Ji patent with the teachings of the Touboul 194 patent because the Touboul 194 patent, like the Ji patent (1:3-6), is directed toward detecting and blocking computer viruses and other malicious code attacks. Touboul 194 Abstract; 1:23-27. The Touboul 194 patent discloses, in addition to Java applets and ActiveX controls, the detection and prevention of both Java Script and Visual Basic attacks. Touboul 194 at Abstract ("The Downloadable may include a Java™ applet. An ActiveX™ control, a JavaScript™ script, or a Visual Basic script.").
5. The computer-based method of claim 1 wherein suspicious computer operations include calls made to an operating system, a file system, a network system, and to memory.	The Ji patent inherently discloses the method wherein the suspicious computer operations include calls made to an operating system, a file system, a network system and to memory. The Ji patent discloses a method that detects all suspicious instructions. The Ji patent discloses scanning the downloaded file to identify "suspicious instructions" (Ji at 5:22) contained in the downloadable as it is received at the server. Ji at 5:16-6:37 ("Examples of pre- and post-monitor functions are: (1) to disallow any directory listing access: pre-filter(function_name, parameters) { if (function_name = =

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
	"java.io.File.list") throw new SecurityException(); } post-filter(result) { }"). Accordingly, this instrumentation (deriving) identifies specific applet instructions deemed to be "suspicious" (computer operations) as determined by "a predefined set of [insecure] functions." Ji at 5:22-23. Moreover, during the instrumentation process, all potentially suspicious computer operations are identified and listed because the Ji patent discloses a process whereby all Java class files that may be called by the downloadable are scanned and instrumented: "An applet pre-fetcher component 38 fetches from the Internet 10 all the dependency files required by a Java class file, if they are not already packed into a JAR file. This is important because the goal is to attach the scanner monitor package to a session only once. A Java applet may contain more than one code module, or class file. Heretofore this disclosure has assumed that all the class files are packed in one JAR file and downloaded once. One monitoring package is attached to the JAR file and every instantiation of this package on the client web browser 22 marks a unique session. However, if the class files are not packed together and are downloaded on an as-needed basis during applet execution, multiple instrumentation will occur and multiple instances of the monitoring package for the same session are created on the client. This creates a problem of how to maintain information on session states. To solve this problem, the pre-fetcher 38 pre-fetches the dependency class files during the static scanning of the main applet code module. The dependency class files are (see below) instrumented once, packed together, and delivered to the client." Ji at 7:8-28. Additionally, it would have been obvious to combine the teachings of the Ji patent with the Touboul 194 patent. The Touboul 194 patent discloses detecting suspicious computer instructions wherein the calls are made to an operating system, a file system, a network system, and to memory. Touboul 194 at 9:37-42 ("The code scanner 325 in step 720 registers the commands and command parameters into a format based on command class (e.g., file operations, network operations, registry operations, operating system operations, resource usage thresholds)..").

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
6. The computer-based method of claim 1 wherein the Downloadable security profile data includes a URL from where the Downloadable originated.	The Ji patent inherently discloses the method step wherein the downloadable security profile data includes a URL from there the downloadable originated. Because the applet (downloadable) is received by a HTTP proxy server with the URL of the originating web server included in the downloaded applet. The applet is subsequently scanned, instrumented and then sent to the web browser on the requesting client computer (see Fig. 1 of the Ji patent): "Upon receipt of a particular Java applet, the HTTP proxy server 32, which is software running on server machine 20 and which has associated scanner software 26, then scans the applet and instruments it using an instrumenter 28 which is part of the scanner software 26. (Downloaded non-applets are not scanned.) The instrumented applet is subject to a special digital signer which is an (optional) part of the scanner 26. The scanned (instrumented) applet, which has been digitally signed is then downloaded to the web browser 22 in the client 14." Ji at 4:66-5:8. Additionally, it would have been obvious to combine the teachings of the Touboul 194 patent with the Ji patent to perform the method step wherein the downloadable security profile data includes a URL from where the downloadable originated. The Touboul 194 patent discloses the inclusion of a URL as part of the security profile data in claim 5: "The method of claim 1, further comprising the step of comparing the URL from which the Downloadable originated against a known URL." Touboul 194 at 10:28-30. The Touboul 194 patent also discloses a URL comparator in claim 58: "The system of claim 32. further comprising a URL comparator coupled to the comparator for comparing the URL from which the Downloadable originated against a known URL." Touboul 194 at 12:52-55.
7. The computer-based method of claim 1 wherein the appended Downloadable includes a digital certificate.	The Ji patent discloses the method step wherein the appended downloadable includes a digital certificate. As the specification discloses: "Next, packer 50 creates a new JAR file (JAR') from the instrumented class files and the monitoring package. The digital signer component 58 digitally signs the applet (now JAR"), with a digital signature unique to the particular scanner 26, for authentication in the local domain. The applet JAR" is then transferred to the client machine 14 for execution."

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
	Ji at 8:4-10.
8. The computer-based method of claim 1 wherein said deriving Downloadable security profile data comprises disassembling the incoming Downloadable.	The Ji patent discloses the method step wherein the deriving of the suspicious instructions (downloadable security profile data) comprises disassembling the incoming applet (downloadable). The Ji patent discloses scanning the downloaded file to identify "suspicious instructions" (Ji at 5:22) contained in the downloadable as it is received at the server (as explained in detail in Ji at 5:16-6:37) requires disassembling the Java code in the applet to instrument the applet with pre- and post-filter interrupts. Additionally, it would have been obvious to combine the Ji patent with the teachings of the Touboul 194 patent. The Touboul 194 patent teaches disassembling the downloadable to derive the downloadable security profile data. Touboul 194 at 9:22-24 ("Method 628 begins in step 705 with the code scanner 325 disassembling the machine code or the Downloadable.")
17. A computer-based method, comprising the steps of:	The Ji patent discloses the preamble. Ji discloses computer implemented applications executing on a computer network. Specifically, the Abstract discloses a "network scanner for security checking of application programs […] received over the Internet or an Intranet has both static (pre-run time) and dynamic (run time) scanning. […] During run time at the client, the instrumented instructions are thereby monitored for security policy violations, and execution of an instruction is prevented in the event of such a violation." Figure 1 of the Ji patent discloses a server and client computer device. It is well understood that a computer includes one or more processors for executing software applications.
receiving an incoming Downloadable;	The Ji patent discloses the step of receiving an incoming downloadable. The Ji patent discloses receiving files "(e.g. Java applets or ActiveX controls)" from the Internet at the server in Fig. 1. See also Ji patent at 3:17-23 ("Thereby in accordance with the invention a scanner (for a virus or other malicious code) provides both static and dynamic scanning for application programs, e.g. Java applets or ActiveX controls. The applets or controls (hereinafter collectively referred to as applets) are conventionally received from e.g. the Internet or an Intranet at a conventional server.").
deriving security profile data for the Downloadable, including a list of suspicious computer operations that may	The Ji patent discloses deriving security profile data for the downloadable, including a list of suspicious computer operations that may be attempted by the downloadable. The Ji patent discloses scanning the downloaded file to identify

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
be attempted by the Downloadable; and	"suspicious instructions" (Ji at 5:22) contained in the downloadable as it is received at the server. Ji at 5:16-6:37. Accordingly, this instrumentation (deriving) identifies specific applet instructions deemed to be "suspicious" (computer operations) as determined by "a predefined set of [insecure] functions." Ji at 5:22-23. Moreover, during the instrumentation process, all potentially suspicious computer operations are identified and listed because the Ji patent discloses a process whereby all Java class files that may be called by the downloadable are scanned and instrumented: "An applet pre-fetcher component 38 fetches from the Internet 10 all the dependency files required by a Java class file, if they are not already packed into a JAR file. This is important because the goal is to attach the scanner monitor package to a session only once. A Java applet may contain more than one code module, or class file. Heretofore this disclosure has assumed that all the class files are packed in one JAR file and downloaded once. One monitoring package is attached to the JAR file and every instantiation of this package on the client web browser 22 marks a unique session. However, if the class files are not packed together and are downloaded on an as-needed basis during applet execution, multiple instrumentation will occur and multiple instances of the monitoring package for the same session are created on the client. This creates a problem of how to maintain information on session states. To solve this problem, the pre-fetcher 38 pre-fetches the dependency class files during the static scanning of the main applet code module. The dependency class files are (see below) instrumented once, packed together, and delivered to the client." Ji at 7:8-28. Additionally, it would have been obvious to combine the disclosures of the Ji patent with the teachings in the Touboul 194 patent relating to deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable. The Touboul 194 patent teaches deriving downloadable security profile data: "[…] the code scanner 325 resolves the DSP data 310. That is, the code scanner 325 uses conventional parsing techniques to decompose the code (including all prefetched

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
	components) of the Downloadable into the DSP data 310. DSP data 310 includes the list of all potentially hostile or suspicious computer operations that may be attempted by a specific Downloadable 307, and may also include the respective arguments of these operations." Touboul 194 at 5:41-48.
transmitting the Downloadable and a representation of the Downloadable security profile data to a destination computer, via a transport protocol transmission.	The Ji patent discloses the step of transmitting the instrumented applet (appended downloadable) to the destination computer via a network that uses a transport protocol, such as TCP/IP (transmission control protocol/Internet protocol). After the applet code has been instrumented at the server, "[t]he instrumented applet is then downloaded from the server to the client (local computer), at which time the applet code is conventionally interpreted by the client Web browser and it begins to be executed. As the applet code is executed, each instrumented instruction is monitored by the Web browser using a monitor package which is part of the scanner and delivered to the client side. Upon execution, each instrumented instruction is subject to a security check. If the security policy (which has been pre-established) is violated, that particular instruction which violates the security policy is not executed, and instead a report is made and execution continues, if appropriate, with the next instruction." Ji at 3:32-44. The Ji patent explains that, as depicted in Fig. 1, the security monitoring package and security policies are included with the instrumented downloadable "in a single JAR (Java archive) file format at the server **32**, and downloaded to the web browser **22** in client machine **14**." Ji at 6:38-42. Regarding the "transport protocol transmission" claim element, the use of a transport protocol to transmit the applet from a HTTP proxy server to the client (destination) computer via the network is inherently disclosed because a person of ordinary skill in the art would understand that network transmissions necessarily require a transport protocol to function. Accordingly, the Ji patent's disclosure of transmitting the single JAR archive file containing the instrumented applet disclosed a transport protocol transmission.
18. The computer-based method of claim 17 wherein the transport protocol is an application transport protocol, and wherein the Downloadable security	The Ji patent discloses the method step wherein the transport protocol is an application transport protocol, and wherein the Downloadable security profile data is inserted as a header within the transport protocol transmission. Regarding "the transport protocol is an application transport

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
profile data is inserted as a header within the transport protocol transmission.	protocol" claim element, as explained in dependent claim 19, which depends from claim 18, HTTP is a transport application protocol. Accordingly, as shown in Figure 1 of the Ji patent, the scanner runs on the HTTP proxy server. And the instrumented applet is downloaded from the HTTP proxy server to the requesting web browser on the client machine: "Upon receipt of a particular Java applet, the HTTP proxy server 32, which is software running on server machine 20 and which has associated scanner software 26, then scans the applet and instruments it using an instrumenter 28 which is part of the scanner software 26. (Downloaded non-applets are not scanned.) The instrumented applet is subject to a special digital signer which is an (optional) part of the scanner 26. The scanned (instrumented) applet, which has been digitally signed is then downloaded to the web browser 22 in the client 14." Ji at 4:66-5:8 Regarding the "downloadable security profile data is inserted as a header within the transport protocol transmission" claim element, the Ji patent inherently discloses this claim element because the URL (which is part of the downloadable security profile data as claimed by the Edery 086 patent in claim 6) is included in the header file. "Upon receipt of a particular Java applet, the HTTP proxy server 32, which is software running on server machine 20 and which has associated scanner software 26, then scans the applet and instruments it using an instrumenter 28 which is part of the scanner software 26. (Downloaded non-applets are not scanned.) The instrumented applet is subject to a special digital signer which is an (optional) part of the scanner 26. The scanned (instrumented) applet, which has been digitally signed is then downloaded to the web browser 22 in the client 14." Ji at 4:66-5:8.
19. The computer-based method of claim 18 wherein the application transport protocol is HTTP.	The Ji patent discloses the method step wherein the application transport protocol is HTTP. As shown in Figure 1 of the Ji patent, the scanner runs on the HTTP proxy server. And the instrumented applet is downloaded from the HTTP proxy server to the requesting web browser on the client machine: "Upon receipt of a particular Java applet, the HTTP proxy server 32, which is software running on server machine 20 and which has associated scanner software 26, then scans the applet and instruments it using an instrumenter 28 which is part of the scanner software 26. (Downloaded non-applets are not scanned.) The instrumented applet is subject to a special digital signer which is an (optional) part of the scanner 26. The

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
	scanned (instrumented) applet, which has been digitally signed is then downloaded to the web browser 22 in the client 14." Ji at 4:66-5:8
20. The computer-based method of claim 18 wherein the application transport protocol is FTP.	The Ji patent inherently discloses the method step wherein the application transport protocol is FTP because the instrumented applet is downloaded to the requesting client computer's web browser. In addition to the HTTP protocol, web browsers support execution of the FTP protocol too.
21. The computer-based method of claim 17 wherein the transport protocol is a network transport protocol, and wherein the Downloadable security profile data is inserted as a frame within the transport protocol transmission.	The Ji patent inherently discloses the method step wherein the transport protocol is a network transport protocol, and wherein the Downloadable security profile data is inserted as a frame within the transport protocol transmission. Per dependent claim 22 (which depends from claim 21), TCP/IP is a network transport protocol. TCP/IP is a network protocol supported by the Windows and Linux operating systems. TCP/IP uses frames for transporting information. Accordingly, the downloadable security profile data must be transported via frames because all information transported using the TCP/IP protocol uses frames.
22. The computer-based method of claim 21 wherein the network transport protocol is TCP/IP.	The Ji patent inherently discloses the method step wherein the network transport protocol is TCP/IP. TCP/IP is a network protocol supported by the Windows and Linux operating systems.
23. The computer-based method of claim 21 wherein the network transport protocol is UDP.	The Ji patent inherently discloses the method step wherein the network transport protocol is UDP. As one of skill in the art at the time would have known, UDP is a network protocol supported by the Windows and Linux operating systems.
31. A computer-based method, comprising the steps of:	The Ji patent discloses the preamble. Ji discloses computer implemented applications executing on a computer network. Specifically, the Abstract discloses a "network scanner for security checking of application programs […] received over the Internet or an Intranet has both static (pre-run time) and dynamic (run time) scanning. […] During run time at the client, the instrumented instructions are thereby monitored for security policy violations, and execution of an instruction is prevented in the event of such a violation." Figure 1 of the Ji patent discloses a server and client computer device. It is well understood that a computer includes one or more processors for executing software applications.
receiving an incoming Downloadable;	The Ji patent discloses the step of receiving an incoming downloadable. The Ji patent discloses receiving files "(e.g. Java applets or ActiveX controls)" from the Internet at the server in Fig. 1. See also Ji patent at 3:17-23 ("Thereby in accordance with the invention a scanner (for a virus or other malicious

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
	code) provides both static and dynamic scanning for application programs, e.g. Java applets or ActiveX controls. The applets or controls (hereinafter collectively referred to as applets) are conventionally received from e.g. the Internet or an Intranet at a conventional server.").
receiving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable;	The Ji patent discloses receiving security profile data for the downloadable, including a list of suspicious computer operations that may be attempted by the downloadable. The Ji patent discloses scanning the downloaded file to identify "suspicious instructions" (Ji at 5:22) contained in the downloadable as it is received at the server. Ji at 5:16-6:37. Accordingly, this instrumentation (deriving) identifies specific applet instructions deemed to be "suspicious" (computer operations) as determined by "a predefined set of [insecure] functions." Ji at 5:22-23. Moreover, during the instrumentation process, all potentially suspicious computer operations are identified and listed because the Ji patent discloses a process whereby all Java class files that may be called by the downloadable are scanned and instrumented: "An applet pre-fetcher component 38 fetches from the Internet 10 all the dependency files required by a Java class file, if they are not already packed into a JAR file. This is important because the goal is to attach the scanner monitor package to a session only once. A Java applet may contain more than one code module, or class file. Heretofore this disclosure has assumed that all the class files are packed in one JAR file and downloaded once. One monitoring package is attached to the JAR file and every instantiation of this package on the client web browser 22 marks a unique session. However, if the class files are not packed together and are downloaded on an as-needed basis during applet execution, multiple instrumentation will occur and multiple instances of the monitoring package for the same session are created on the client. This creates a problem of how to maintain information on session states. To solve this problem, the pre-fetcher 38 pre-fetches the dependency class files during the static scanning of the main applet code module. The dependency class files are (see below) instrumented once, packed together, and delivered to the client." Ji at 7:8-28.

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
	Additionally, it would have been obvious to combine the disclosures of the Ji patent with the teachings in the Touboul 194 patent relating to deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable. The Touboul 194 patent teaches deriving downloadable security profile data: "[…] the code scanner 325 resolves the DSP data 310. That is, the code scanner 325 uses conventional parsing techniques to decompose the code (including all prefetched components) of the Downloadable into the DSP data 310. DSP data 310 includes the list of all potentially hostile or suspicious computer operations that may be attempted by a specific Downloadable 307, and may also include the respective arguments of these operations." Touboul 194 at 5:41-48. Further, it would have been obvious to combine the Ji patent with the teaching of the Touboul 194 patent to retrieve security profile data for the incoming applet (downloadable) from a database of downloadable security profiles indexed according to downloadable IDs, based on an ID of the incoming downloadable, the security profile data including a list of suspicious computer operations that may be attempted by the Downloadable. The Touboul 194 patent discloses the use of downloadable IDs for known downloadables. Touboul 194 at 5:4-6 ("The first comparator 320 receives the Downloadable, the Downloadable ID and the security policy 305 from the policy finder 317."). Additionally, the Touboul 194 patent discloses retrieving security profile data that includes a list of suspicious computer operations that may be attempted by the downloadable. "[…] the ID generator 315 may retrieve all components listed in the .INF file for an ActiveXTM control to compule a Downloadable 10. Accordingly, the Downloadable ID for the Downloadable will be the same eacb time the ID generator 315 receives the same Downloadable. The ID generator 315 adds the generated Downloadable ID to the list of known Downloadables 307 (if it is not already listed) The ID generator 315 then forwards the Downloadable and Downloadable ID to the policy finder 317." Touboul 194 at 4:52-61.
appending a representation of the Downloadable security profile data to the Downloadable, to generate an appended Downloadable;	The Ji patent discloses the step of appending a representation of the Downloadable security profile data to the Downloadable, to generate an appended Downloadable. Specifically, the Ji patent discloses generating the amended downloadable by instrumenting (appending) all of the "suspicious instructions"

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
and	(downloadable security profile data) in the applet (downloadable). Ji at 5:16-6:37. Additionally, the Ji patent discloses at 7:8-28 (1) downloading "dependency" Java class files not included in the applet (downloadable) but required by the applet during execution; (2) instrumenting the newly downloaded Java class files to derive suspicious instructions (downloadable security profile data) included therein; and (3) appending to the downloadable the instrumented Java class files: "**An applet pre-fetcher component 38 fetches from the Internet 10 all the dependency files required by a Java class file**, if they are not already packed into a JAR file. This is important because the goal is to attach the scanner monitor package to a session only once. A Java applet may contain more than one code module, or class file. Heretofore this disclosure has assumed that all the class files are packed in one JAR file and downloaded once. One monitoring package is attached to the JAR file and every instantiation of this package on the client web browser 22 marks a unique session. However, if the class files are not packed together and are downloaded on an as-needed basis during applet execution, multiple instrumentation will occur and multiple instances of the monitoring package for the same session are created on the client. This creates a problem of how to maintain information on session states. To solve this problem, **the pre-fetcher 38 pre-fetches the dependency class files during the static scanning of the main applet code module. The dependency class files are (see below) instrumented once, packed together, and delivered to the client.**" Ji at 7:8-28 (emphasis added). The Ji patent further explains that, as depicted in Fig. 1, the security monitoring package and security policies are included with the instrumented downloadable (and the instrumented Java class files) "in a single JAR (Java archive) file format at the server **32**, and downloaded to the web browser **22** in client machine **14**." Ji at 6:38-42.
transmitting the appended Downloadable to a	The Ji patent discloses the step of transmitting the instrumented applet (appended downloadable) to the destination computer.

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
destination computer.	After the applet code has been instrumented at the server, "[t]he instrumented applet is then downloaded from the server to the client (local computer), at which time the applet code is conventionally interpreted by the client Web browser and it begins to be executed. As the applet code is executed, each instrumented instruction is monitored by the Web browser using a monitor package which is part of the scanner and delivered to the client side. Upon execution, each instrumented instruction is subject to a security check. If the security policy (which has been pre-established) is violated, that particular instruction which violates the security policy is not executed, and instead a report is made and execution continues, if appropriate, with the next instruction." Ji at 3:32-44. The Ji patent explains that, as depicted in Fig. 1, the security monitoring package and security policies are included with the instrumented downloadable "in a single JAR (Java archive) file format at the server **32**, and downloaded to the web browser **22** in client machine **14**." Ji at 6:38-42.
32. The computer-based method of claim 31 further comprising forwarding the Downloadable to an external computer, for deriving the Downloadable security profile data.	The Ji patent discloses the method step comprising forwarding the downloadable to an external computer for deriving the downloadable security profiled data. Specifically, the Ji patent discloses for Figure 1 that "[t]he security policy generator 54 may run on server machine 20 **or another computer**." Ji at 7:53-55 (emphasis added).
35. A computer-based method, comprising the steps of:	The Ji patent discloses the preamble. Ji discloses computer implemented applications executing on a computer network. Specifically, the Abstract discloses a "network scanner for security checking of application programs […] received over the Internet or an Intranet has both static (pre-run time) and dynamic (run time) scanning. […] During run time at the client, the instrumented instructions are thereby monitored for security policy violations, and execution of an instruction is prevented in the event of such a violation." Figure 1 of the Ji patent discloses a server and client computer device. It is well understood that a computer includes one or more processors for executing software applications.
receiving an incoming Downloadable;	The Ji patent discloses the step of receiving an incoming downloadable. The Ji patent discloses receiving files "(e.g. Java applets or ActiveX controls)" from the Internet at the server in Fig. 1. See also Ji patent at 3:17-23 ("Thereby in accordance with the invention a scanner (for a virus or other malicious

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
	code) provides both static and dynamic scanning for application programs, e.g. Java applets or ActiveX controls. The applets or controls (hereinafter collectively referred to as applets) are conventionally received from e.g. the Internet or an Intranet at a conventional server.”).
receiving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and	The Ji patent discloses receiving security profile data for the downloadable, including a list of suspicious computer operations that may be attempted by the downloadable. The Ji patent discloses scanning the downloaded file to identify “suspicious instructions” (Ji at 5:22) contained in the downloadable as it is received at the server. Ji at 5:16-6:37. Accordingly, this instrumentation (deriving) identifies specific applet instructions deemed to be “suspicious” (computer operations) as determined by “**a predefined set of [insecure] functions.**” Ji at 5:22-23 (emphasis added). Moreover, during the instrumentation process, all potentially suspicious computer operations are identified and listed because the Ji patent discloses a process whereby all Java class files that may be called by the downloadable are scanned and instrumented: “An applet pre-fetcher component 38 fetches from the Internet 10 all the dependency files required by a Java class file, if they are not already packed into a JAR file. This is important because the goal is to attach the scanner monitor package to a session only once. A Java applet may contain more than one code module, or class file. Heretofore this disclosure has assumed that all the class files are packed in one JAR file and downloaded once. One monitoring package is attached to the JAR file and every instantiation of this package on the client web browser 22 marks a unique session. However, if the class files are not packed together and are downloaded on an as-needed basis during applet execution, multiple instrumentation will occur and multiple instances of the monitoring package for the same session are created on the client. This creates a problem of how to maintain information on session states. To solve this problem, the pre-fetcher 38 pre-fetches the dependency class files during the static scanning of the main applet code module. The dependency class files are (see below) instrumented once, packed together, and delivered to the client.” Ji at 7:8-28.

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
	Additionally, it would have been obvious to combine the disclosures of the Ji patent with the teachings in the Touboul 194 patent relating to deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable. The Touboul 194 patent teaches deriving downloadable security profile data: "[…] the code scanner 325 resolves the DSP data 310. That is, the code scanner 325 uses conventional parsing techniques to decompose the code (including all prefetched components) of the Downloadable into the DSP data 310. DSP data 310 includes the list of all potentially hostile or suspicious computer operations that may be attempted by a specific Downloadable 307, and may also include the respective arguments of these operations." Touboul 194 at 5:41-48. Further, it would have been obvious to combine the Ji patent with the teaching of the Touboul 194 patent to retrieve security profile data for the incoming applet (downloadable) from a database of downloadable security profiles indexed according to downloadable IDs, based on an ID of the incoming downloadable, the security profile data including a list of suspicious computer operations that may be attempted by the Downloadable. The Touboul 194 patent discloses retrieving security profile data that includes a list of suspicious computer operations that may be attempted by the downloadable. "[…] the ID generator 315 may retrieve all components listed in the .INF file for an ActiveXTM control to compule a Downloadable 10. Accordingly, the Downloadable ID for the Downloadable will be the same eacb time the ID generator 315 receives the same Downloadable. The ID generator 315 adds the generated Downloadable ID to the list of known Downloadables 307 (if it is not already listed) The ID generator 315 then forwards the Downloadable and Downloadable ID to the policy finder 317." Touboul 194 at 4:52-61.
transmitting the Downloadable and a representation of the Downloadable security profile data to a destination computer, via a transport protocol transmission.	The Ji patent discloses the step of transmitting the instrumented applet (appended downloadable) to the destination computer via a network that uses a transport protocol, such as TCP/IP (transmission control protocol/Internet protocol). After the applet code has been instrumented at the server, "[t]he instrumented applet is then downloaded from the server to the client (local computer), at which time the applet code is conventionally interpreted by the client Web browser and it begins to be executed. As the applet code is executed, each instrumented instruction is monitored by the Web browser using

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
	a monitor package which is part of the scanner and delivered to the client side. Upon execution, each instrumented instruction is subject to a security check. If the security policy (which has been pre-established) is violated, that particular instruction which violates the security policy is not executed, and instead a report is made and execution continues, if appropriate, with the next instruction." Ji at 3:32-44. The Ji patent explains that, as depicted in Fig. 1, the security monitoring package and security policies are included with the instrumented downloadable "in a single JAR (Java archive) file format at the server **32**, and downloaded to the web browser **22** in client machine **14**." Ji at 6:38-42. Regarding the "transport protocol transmission" claim element, the use of a transport protocol to transmit the applet from a HTTP proxy server to the client (destination) computer via the network is inherently disclosed because a person of ordinary skill in the art would understand that network transmissions necessarily require a transport protocol to function. Accordingly, the Ji patent's disclosure of transmitting the single JAR archive file containing the instrumented applet disclosed a transport protocol transmission.
36. The computer-based method of claim 35 further comprising forwarding the Downloadable to an external computer, for deriving the Downloadable security profile data.	The Ji patent discloses the method step comprising forwarding the downloadable to an external computer for deriving the downloadable security profiled data. Specifically, the Ji patent discloses for Figure 1 that "[t]he security policy generator 54 may run on server machine 20 **or another computer**." Ji at 7:53-55 (emphasis added).
39. A computer-based method, comprising the steps of:	The Ji patent discloses the preamble. Ji discloses computer implemented applications executing on a computer network. Specifically, the Abstract discloses a "network scanner for security checking of application programs […] received over the Internet or an Intranet has both static (pre-run time) and dynamic (run time) scanning. […] During run time at the client, the instrumented instructions are thereby monitored for security policy violations, and execution of an instruction is prevented in the event of such a violation." Figure 1 of the Ji patent discloses a server and client computer device. It is well understood that a computer includes one or more processors for executing software applications.
receiving an incoming	The Ji patent discloses the step of receiving an incoming

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
Downloadable;	downloadable. The Ji patent discloses receiving files "(e.g. Java applets or ActiveX controls)" from the Internet at the server in Fig. 1. See also Ji patent at 3:17-23 ("Thereby in accordance with the invention a scanner (for a virus or other malicious code) provides both static and dynamic scanning for application programs, e.g. Java applets or ActiveX controls. The applets or controls (hereinafter collectively referred to as applets) are conventionally received from e.g. the Internet or an Intranet at a conventional server.").
retrieving security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to Downloadable IDs, based on an ID of the incoming Downloadable, the security profile data including a list of suspicious computer operations that may be attempted by the Downloadable;	It would have been obvious to combine the Ji patent with the teaching of the Touboul 194 patent to retrieve security profile data for the incoming applet (downloadable) from a database of downloadable security profiles indexed according to downloadable IDs, based on an ID of the incoming downloadable, the security profile data including a list of suspicious computer operations that may be attempted by the Downloadable. The Touboul 194 patent discloses the use of downloadable IDs for known downloadables. Touboul 194 at 5:4-6 ("The first comparator 320 receives the Downloadable, the Downloadable ID and the security policy 305 from the policy finder 317."). Additionally, the Touboul 194 patent discloses retrieving security profile data that includes a list of suspicious computer operations that may be attempted by the downloadable. "[…] the ID generator 315 may retrieve all components listed in the .INF file for an ActiveXTM control to compule a Downloadable 10. Accordingly, the Downloadable ID for the Downloadable will be the same eacb time the ID generator 315 receives the same Downloadable. The ID generator 315 adds the generated Downloadable ID to the list of known Downloadables 307 (if it is not already listed) The ID generator 315 then forwards the Downloadable and Downloadable ID to the policy finder 317." Touboul 194 at 4:52-61.
appending a representation of the retrieved Downloadable security profile data to the incoming Downloadable, to generate an appended Downloadable; and	The Ji patent discloses the step of appending a representation of the Downloadable security profile data to the Downloadable, to generate an appended Downloadable. Specifically, the Ji patent discloses generating the amended downloadable by instrumenting (appending) all of the "suspicious instructions" (downloadable security profile data) in the applet (downloadable). Ji at 5:16-6:37. Additionally, the Ji patent discloses at 7:8-28 (1) downloading "dependency" Java class files not included in the applet (downloadable) but required by the applet during execution; (2)

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
	instrumenting the newly downloaded Java class files to derive suspicious instructions (downloadable security profile data) included therein; and (3) appending to the downloadable the instrumented Java class files: "**An applet pre-fetcher component 38 fetches from the Internet 10 all the dependency files required by a Java class file**, if they are not already packed into a JAR file. This is important because the goal is to attach the scanner monitor package to a session only once. A Java applet may contain more than one code module, or class file. Heretofore this disclosure has assumed that all the class files are packed in one JAR file and downloaded once. One monitoring package is attached to the JAR file and every instantiation of this package on the client web browser 22 marks a unique session. However, if the class files are not packed together and are downloaded on an as-needed basis during applet execution, multiple instrumentation will occur and multiple instances of the monitoring package for the same session are created on the client. This creates a problem of how to maintain information on session states. To solve this problem, **the pre-fetcher 38 pre-fetches the dependency class files during the static scanning of the main applet code module. The dependency class files are (see below) instrumented once, packed together, and delivered to the client.**" Ji at 7:8-28 (emphasis added). The Ji patent further explains that, as depicted in Fig. 1, the security monitoring package and security policies are included with the instrumented downloadable (and the instrumented Java class files) "in a single JAR (Java archive) file format at the server **32**, and downloaded to the web browser **22** in client machine **14**." Ji at 6:38-42.
transmitting the appended Downloadable to a destination computer.	The Ji patent discloses the step of transmitting the instrumented applet (appended downloadable) to the destination computer via a network that uses a transport protocol, such as TCP/IP (transmission control protocol/Internet protocol). After the applet code has been instrumented at the server, "[t]he instrumented applet is then downloaded from the server to the client (local computer), at which time the applet code is conventionally interpreted by the client Web browser and it

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
	begins to be executed. As the applet code is executed, each instrumented instruction is monitored by the Web browser using a monitor package which is part of the scanner and delivered to the client side. Upon execution, each instrumented instruction is subject to a security check. If the security policy (which has been pre-established) is violated, that particular instruction which violates the security policy is not executed, and instead a report is made and execution continues, if appropriate, with the next instruction." Ji at 3:32-44. The Ji patent explains that, as depicted in Fig. 1, the security monitoring package and security policies are included with the instrumented downloadable "in a single JAR (Java archive) file format at the server **32**, and downloaded to the web browser **22** in client machine **14**." Ji at 6:38-42.
41. A computer-based method, comprising the steps of:	The Ji patent discloses the preamble. Ji discloses computer implemented applications executing on a computer network. Specifically, the Abstract discloses a "network scanner for security checking of application programs […] received over the Internet or an Intranet has both static (pre-run time) and dynamic (run time) scanning. […] During run time at the client, the instrumented instructions are thereby monitored for security policy violations, and execution of an instruction is prevented in the event of such a violation." Figure 1 of the Ji patent discloses a server and client computer device. It is well understood that a computer includes one or more processors for executing software applications.
receiving an incoming Downloadable;	The Ji patent discloses the step of receiving an incoming downloadable. The Ji patent discloses receiving files "(e.g. Java applets or ActiveX controls)" from the Internet at the server in Fig. 1. See also Ji patent at 3:17-23 ("Thereby in accordance with the invention a scanner (for a virus or other malicious code) provides both static and dynamic scanning for application programs, e.g. Java applets or ActiveX controls. The applets or controls (hereinafter collectively referred to as applets) are conventionally received from e.g. the Internet or an Intranet at a conventional server.").
retrieving security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to Downloadable	It would have been obvious to combine the Ji patent with the teaching of the Touboul 194 patent to retrieve security profile data for the incoming applet (downloadable) from a database of downloadable security profiles indexed according to downloadable IDs, based on an ID of the incoming downloadable, the security profile data including a list of

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
IDs, based on an ID of the incoming Downloadable, the security profile data including a list of suspicious computer operations that may be attempted by the Downloadable; and	suspicious computer operations that may be attempted by the Downloadable. The Touboul 194 patent discloses the use of downloadable IDs for known downloadables. Touboul 194 at 5:4-6 ("The first comparator 320 receives the Downloadable, the Downloadable ID and the security policy 305 from the policy finder 317."). Additionally, the Touboul 194 patent discloses retrieving security profile data that includes a list of suspicious computer operations that may be attempted by the downloadable. "the ID generator 315 may retrieve all components listed in the .INF file for an ActiveXTM control to compule a Downloadable 10. Accordingly, the Downloadable ID for the Downloadable will be the same eacb time the ID generator 315 receives the same Downloadable. The ID generator 315 adds the generated Downloadable ID to the list of known Downloadables 307 (if it is not already listed) The ID generator 315 then forwards the Downloadable and Downloadable ID to the policy finder 317." Touboul 194 at 4:52-61.
transmitting the incoming Downloadable and a representation of the retrieved Downloadable security profile data to a destination computer, via a transport protocol transmission.	The Ji patent discloses the step of transmitting the instrumented applet (downloadable and downloadable security profile) to the destination computer via a network that uses a transport protocol, such as TCP/IP (transmission control protocol/Internet protocol). After the applet code has been instrumented at the server, "[t]he instrumented applet is then downloaded from the server to the client (local computer), at which time the applet code is conventionally interpreted by the client Web browser and it begins to be executed. As the applet code is executed, each instrumented instruction is monitored by the Web browser using a monitor package which is part of the scanner and delivered to the client side. Upon execution, each instrumented instruction is subject to a security check. If the security policy (which has been pre-established) is violated, that particular instruction which violates the security policy is not executed, and instead a report is made and execution continues, if appropriate, with the next instruction." Ji at 3:32-44. The Ji patent explains that, as depicted in Fig. 1, the security monitoring package and security policies are included with the instrumented downloadable "in a single JAR (Java archive) file format at the server **32**, and downloaded to the web browser **22** in client machine **14**." Ji at 6:38-42. Regarding the "transport protocol transmission" claim element, the use of a transport protocol to transmit the applet from a

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul 194 Patent
	HTTP proxy server to the client (destination) computer via the network is inherently disclosed because a person of ordinary skill in the art would understand that network transmissions necessarily require a transport protocol to function. Accordingly, the Ji patent's disclosure of transmitting the single JAR archive file containing the instrumented applet disclosed a transport protocol transmission.

V. CONCLUSION

Based on the above remarks, it is respectfully submitted that a substantial new question of patentability has been raised with respect to claims 1, 2, 3, 4, 5, 6, 7, 8, 17, 18, 19, 20, 21, 22, 23, 31, 32, 35, 36, 39 and 41 of the Edery 086 patent. Therefore, reexamination of claims 1, 2, 3, 4, 5, 6, 7, 8, 17, 18, 19, 20, 21, 22, 23, 31, 32, 35, 36, 39 and 41 is respectfully requested.

Respectfully submitted,

Dated: October 7, 2013

/Ryan W. Cobb/

Ryan W. Cobb
Reg. No. 64,598
Attorney for Requestor

DLA PIPER LLP (US)
401 B Street, Suite 1700
San Diego, CA 92101
ryan.cobb@dlapiper.com
(619) 699-2700
(619) 699-2701

Acknowledgement Receipt

The USPTO has received your submission at **13:34:28** Eastern Time on **07-OCT-2013** by Deposit Account: [redacted]

$ **12000** fee paid by e-Filer via *RAM* with Confirmation Number: 10650.

You have also pre-authorized the following payments from your USPTO Deposit Account:

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

eFiled Application Information

EFS ID	17054023
Application Number	90013015
Confirmation Number	5243
Title	MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS
First Named Inventor	Yigal Mordechai Edery
Customer Number or Correspondence Address	Ryan W. Cobb DLA Piper LLP (US) 401 B Street Suite 1700 San Diego CA 92101 US 619-699-2635 ryan.cobb@dlapiper.com
Filed By	Ryan Cobb
Attorney Docket Number	382984-000006
Filing Date	
Receipt Date	07-OCT-2013
Application Type	Reexam (Third Party)

Application Details

Submitted Files	Page Count	Document Description	File Size	Warnings
01PTOTransmittal086.PDF	2	Transmittal of New Application	46687 bytes	PASS
02USP8079086B1.pdf	27	Copy of patent for which reexamination is requested	1946384 bytes	PASS
03RequestForReexam.pdf	36	Receipt of Orig. Ex Parte Request by Third Party	363421 bytes	PASS
04IDS086.PDF	2	Reexam - Info Disclosure Statement Filed by 3rd Party	64778 bytes	PASS
		Reexam Miscellaneous	652403	

05USP5983348.pdf	9	Incoming Letter	bytes	PASS
06USP6092194.pdf	23	Reexam Miscellaneous Incoming Letter	1124638 bytes	PASS
07CertificateOfService.pdf	1	Reexam Certificate of Service	129340 bytes	PASS
fee-info.pdf	2	Fee Worksheet (SB06)	29720 bytes	PASS

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

If you need help:

- *To ask questions about Patent e-Filing, or to suggest improvements to the online system, or report technical problems, please call the Patent Electronic Business Center at (866) 217-9197 (toll free) or send email to EBC@uspto.gov.*
- *Send general questions about USPTO programs to the USPTO Contact Center (UCC) .*
- *For general questions regarding a petition, or requirements for filing a petition, contact the Office of Petitions Help Desk at 1 800-786-9199.*